Claims

What is claimed is:

1. A method for obtaining an approval of an electronic fund transfer disbursement file from a user of a remote system and transferring the electronic fund transfer disbursement file to a payments processor, the method comprising:

generating a digest by performing a hash on the electronic fund transfer disbursement file;

transferring the digest to the remote system;

transferring authorization control code to the remote system, the authorization control code driving the remote system to perform the following steps:

obtain a digital signature of authenticated attributes, the authenticated attributes including the digest;

generate an authorization response, the authorization response including the digital signature;

receiving the authorization response from the remote system; and

transferring an electronic funds submission to the payments processor, the electronic funds submission comprising the payment transaction file and at least a portion of the authorization response comprising the digital signature.

2. The method of claim 1 wherein:

the authorization control code further provides for the remote system to:

generate additional message attributes; and

combine the additional message attributes with the digest to generate the authenticated attributes; and

the digital signature comprises a digital signature of a hash of the authenticated attributes.

3. The method of claim 2, wherein the authorization control code further drives the

remote system to:

generate and pass a dummy data string to a signing component to obtain a dummy authentication data structure, the dummy authentication data structure comprising a dummy digital signature;

pass the authenticated attributes to the signing component to obtain the digital signature;

combine the digital signature with at least a portion of the dummy authentication data structure by replacing the dummy digital signature with the digital signature to generate an authentication data structure; and

include the authentication data structure in the authorization response.

4. The method of claim 3; wherein:

the dummy data structure further comprises a dummy digest; and

the authorization control code further drives the remote system to combine the digest with the dummy authentication data structure to generate the authentication data structure by replacing the dummy digest with the digest.

5. The method of claim 4:

further comprising authenticating the user of the remote system by:

obtaining logon credentials identifying the user of the remote system;

determining whether the logon credentials match those of an authorized user; and

the step of transferring the authorization request to the remote system occurs only if the logon credentials match those of an authorized user.

6. The method of claim 5, further comprising authenticating the user of the remote system to the payments processor by:

receiving an authentication challenge from the payments processor;

transferring the authentication challenge to the remote system;

receiving an authentication response from the remote system; and

transferring the authentication response to the payments processor.

7. A method for obtaining an approval of an electronic fund transfer disbursement file from a user of a remote system and transferring the electronic fund transfer disbursement file to a payments processor, the method comprising:

generating a digest by performing a hash on the electronic fund transfer disbursement file;

transferring the digest to the remote system;

receiving an authorization response from the remote system, the authorization response comprising a digital signature of authenticated attributes, the authenticated attributes including the digest;

transferring an electronic funds submission to the payments processor over a secure connection, the electronic funds submission comprising the payment transaction file and at least a portion of the authorization response comprising the digital signature.

8. The method of claim 7 wherein:

the authorization control code further provides for the remote system to:

generate additional message attributes; and

combine the additional message attributes with the digest to generate the authenticated attributes; and

the digital signature comprises a digital signature of a hash of the authenticated attributes.

9. The method of claim 8, wherein the remote system:

generates and passes a dummy data file to a signing component to obtain a dummy authentication data structure, the dummy authentication data structure comprising a dummy digital signature;

passes the authenticated attributes to the signing component to obtain the digital signature;

combines the digital signature with at least a portion of the dummy authentication data structure by replacing the dummy digital signature with the digital signature to generate an authentication data structure; and

includes the authentication data structure in the authorization response.

10. The method of claim 9, wherein:

the dummy data structure further comprises a dummy digest; and

the remote system further combines the digest with the dummy authentication data structure to generate the authentication data structure by replacing the dummy digest with the digest.

11. The method of claim 10, further comprising:

authenticating the user of the remote system by:

obtaining logon credentials identifying the user of the remote system;

determining whether the logon credentials match those of an authorized user; and

the step of transferring the authorization request to the remote system occurs only if the logon credentials match those of an authorized user.

12. The method of claim 11, further comprising authenticating the user of the remote system to the payments processor by:

receiving an authentication challenge from the payments processor;

transferring the authentication challenge to the remote system;

receiving an authentication response from the remote system; and

transferring the authentication response to the payments processor.

13. The method of claim 7, further comprising passing authorization control code to the remote system, the authorization control code being at least one of executable by

the remote system and interpretable by the remote system for driving the remote system to:

obtain the digital signature of the authenticated attributes; and

generate the authorization response.

14. The method of claim 13:

the authorization control code further provides for the remote system to:

generate additional message attributes; and

combine the additional message attributes with the digest to generate the authenticated attributes; and

the digital signature comprises a digital signature of a hash of the authenticated attributes.

15. The method of claim 14, wherein the authorization control code further drives the remote system to:

generate and pass a dummy data file to a signing component to obtain a dummy authentication data structure, the dummy authentication data structure comprising a dummy digital signature;

pass the authenticated attributes to the signing component to obtain the digital signature;

combine the digital signature with at least a portion of the dummy authentication data structure by replacing the dummy digital signature with the digital signature to generate an authentication data structure; and

include the authentication data structure in the authorization response.

16. The method of claim 15:

wherein the dummy data structure further comprises a dummy digest; and

the authorization control code further drives the remote system to combine the digest with the dummy authentication data structure to generate the authentication data structure by replacing the dummy digest with the digest.

17. The method of claim 16:

further comprising authenticating the user of the remote system by:

obtaining logon credentials identifying the user of the remote system;

determining whether the logon credentials match those of an authorized user; and

the step of transferring the authorization request to the remote system occurs only if the logon credentials match those of an authorized user.

18. The method of claim 17, further comprising authenticating the user of the remote system to the payments processor by:

receiving an authentication challenge from the payments processor;

transferring the authentication challenge to the remote system;

receiving an authentication response from the remote system; and

transferring the authentication response to the payments processor.